Cooperative Electronic Attack Using Unmanned Air Vehicles

By Dr. Mark J. Mears

Editorial Abstract: Dr. Mears explores electronic attack of integrated air defenses using multiple unmanned air vehicles acting in a coordinated fashion. He begins with an electronic warfare primer, and threat environment outline, then describes the utility of EA against networked radar sites, and offers approaches to solving command and control challenges.

(Editor's note: In an era seemingly dominated by influence operations, we never forget that Electronic Warfare is doctrinally and historically a large part of Information Operations. This article illustrates the ongoing importance of EW research and subsequent real world applications.)

Introduction

In the evolution of warfare, we've developed a number of skills, arts, and sciences. As a method is developed for attacking and effectively exploit enemy weaknesses, they create an associated method of defense to make our attack less effective. Electronic Attack (EA) is a counter-counter-measure to reduce the effectiveness of radar systems, allowing aircraft to fly unharmed among radars and associated missiles. This is done by either distracting the radar with confusing or deceptive information, or by blinding the radar—making it unable to detect, track, engage, or destroy threats. In the past, we've often achieved EA by flying specially designed EW aircraft between a radar site and the shielded strike- configured aircraft. In these cases, the radar may able to determine the direction to the jamming aircraft, but is denied range information and any information about the strike aircraft. The type of EA activity that is the focus of this paper is referred to as non-destructive Suppression of Enemy Air Defenses (SEAD).[1]

In this article, our primary interest is how the EA requirements are part of greater cooperative control requirements. These new considerations are based on coordinated use of multiple unmanned air vehicles (UAVs) for EW. Whereas conventional EA is most often done using a single aircraft working together with one or two other aircraft being hidden from the view of a radar site, here are discussing UAVs working together with each other and groups of protected aircraft. The use of UAVs for any task presents a number of technical challenges, and EA is no exception.

The Threat: Radar & IADS

Radar systems operate on the basic principle of sending out radio frequency (RF) electromagnetic radiation (EM) and then "listening" for the reflected signal from distant targets. A radar's radio signal footprint often has a lobe structure with a large "main beam" or "mainlobe," and many smaller gain directions called "sidelobes," as shown in figure 1. During normal operation the gain of the mainlobe is so much larger

Future electronic attacker? (Defense Link)

than the sidelobes, we generally assume the target is in the same direction the mainlobe is pointed. The direction of the main beam is also referred to as the Line-of-Sight (LOS) and in Figure 1, this angle is denoted by μ. Distance to target can be obtained by measuring the difference between the time of signal transmission and the time of reception of the reflected signal. The range rate can be determined by the Doppler shift of the reflected signal, and we can estimate the angular rate from a sequence of angular measurements (shifts in the direction of the centroid of the mainlobe) of the target. The end result is a measurement of the position and velocity of vehicles within the radar's detection range.[2] The size of this detection range is influenced by radar power limitations, antenna gain, electronic noise and environmental factors. Since the radar is able to point the mainlobe in any direction, we abstract the shape of this region as a circle with the radius of the circle given by the burn-through radius (RB), so noted because the target burns through the noise clutter at that range. This is also referred to as the radar's "threat circle."

Radars are also capable of receiving energy through their sidelobes. However, this effect is undesirable from the radar's point of view. Since the both majority of the EM and largest gain for the returned signal are through the mainlobe, energy received through a sidelobe can cause the radar to indicate an errant or incorrect angle to the target. In order to minimize this effect, many radars can "notch out," or cancel their sidelobes. Today's integrated radar systems are complex networked entities that communicate with other radar units to correlate information, and with missile systems to engage and destroy perceived threats. Various types of radar with tailored characteristics typically make up a defense network

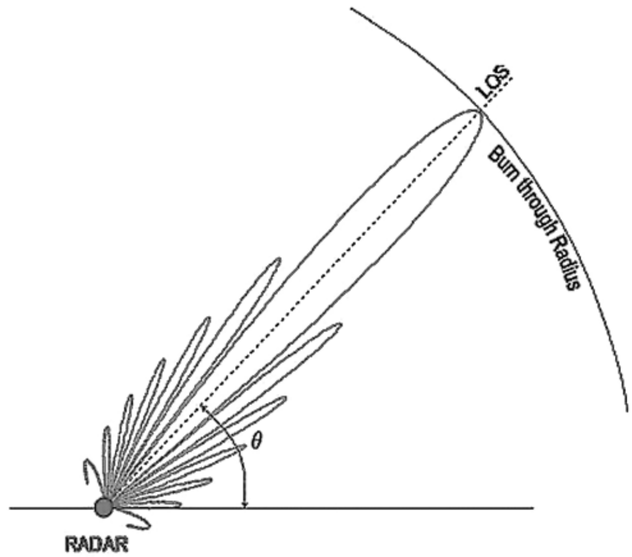

Fig. 1. RADAR Lobe Structure

with a hierarchy that includes early warning, tracking, and terminal guidance radars. The units are geographically placed to defend key assets, and overlap to prevent gaps in coverage. Use of mobile radars that light-up only when prompted by other radars in the network create uncertainty for attackers. Also, we must assume we'll face layers of different radars with communication linkage and geographic coverage to minimize the likelihood an adversary will be able to penetrate defense and escape unharmed.

Each radar unit will also have modes such as lobe structure adjustment, mono-pulse operation, frequency alteration, pulse-repetition-frequency changes, pulse-to-pulse agility, multi-static operation and signal gating to allow precision information gathering.[2] These are only a few of the tools that can be used to prevent adversaries from avoiding detection and destruction. Thus, robustness to counter counter-counter measures is vitally important for our EA methods to be useful. It would certainly be unwise to invest heavily in ”point solutions” that could be easily foiled by simple modifications. While Integrated Air Defense Systems (IADS) offer a number of great topics to explore, we will address only those radar feature considerations needed for coordinated UAV EA.

Electronic Warfare

EW is the use of electromagnetic radiation (EM) to control the EM spectrum, or directed energy to attack an enemy.[3] We further divide it into three main components. Electronic Protection involves passive and active means for preventing adverse impact of EM on combat capability. Electronic Warfare Support (ES) is the subdivision of EW that deals with actions to gather information about sources of adverse EM activity. Electronic Attack (EA) deals with use of EM, directed energy, or anti-radiation missiles to adversely affect enemy combat capability.

EA can also be put in the context of Suppression of Enemy Air Defenses (SEAD), and can be either destructive or disruptive. In military doctrine, destructive SEAD means permanent target destruction. Alternately, disruptive SEAD means temporarily neutralizing radars, thus EA of an IADS can be considered part of it. We can break down SEAD into the following: 1) suppression over a large area, 2) ”localized” suppression of small areas for time intervals, and 3) suppression against targets of opportunity. UAVs have considerable potential to contribute toward all three tasks. Given a large enough UAV fleet, we could persistently cover large areas, and small teams could suppress EM in localized areas for specified times, thereby opening corridors for operations. By leaving teams of UAVs in our areas of interest, our forces could also suppress Time Sensitive Targets (TST).

Electronic means for countering radars, generally referred to as Electronic Countermeasures (ECM), fall into six general categories: 1) use of chaff, 2) gate stealing, 3) angle deception, 4) use of decoys, 5) noise jamming and 6) false target generation. Varied as these radar countermeasures are, cooperative control of UAVs can contribute to EA effectiveness in each category. Chaff effectively increases noise in the radar return signal, and can be used to screen (hide) areas, or in end-game maneuvers in conjunction with evasive maneuvers, to break a missiles seeker's lock.

Chaff is a simple means of ECM, but can be particularly effective in conjunction with other methods. A second method, called Gate Stealing, gradually dominates the true return signal with an artificial signal. In order to maintain good signal to noise ratio of an observed target, radars gate a target's range, speed, or both. Once the radar acquires a strong signal, the operator lowers the gain, and the artificial signal is free to manipulate the radar's perception independent of the activities of the real aircraft.

Another method of dealing with radars is for aircraft to cause a radar to see their image at angles different from the actual Line-of-Sight. This can be implemented by bouncing EM signals from the terrain to the radar, or by altering the shape of the wave front through phase adjustment of EM sent from different places on the aircraft. These methods are referred to as Angle Deception.

We must also examine use of decoys—devices that distract radar by drawing their attention. These can be expendable entities which serve their purpose with no plan for recovery, or towed devices reeled out behind the aircraft to act as false targets—and recovered afterwards. As expendable decoys get more complex, the line between decoy, munition and generic UAV is becoming blurred. However, increased emphasis on mobile radars suggests a primary role will be exposing hidden radar sights, which give away their position by actively responding to the decoys.

Of course, radar counter measures work best when part of a coordinated effort. The characteristics of each ECM type leads to preplanned methods of use. However, in the context of cooperative control, where we're concerned with UAV positioning and movement planning, two ECM methods are of most interest. Noise Jamming is an ECM method where EM energy is transmitted to a radar in order to raise the noise level and make it harder for the radar to extract the signal. This is not covert, since the enemy is immediately aware of a threat. Although the radar will know the signals' Angle of Arrival (AoA), it won't have range or range rate, and therefore will lack fire control information. The need to manage power over both time and frequency ranges results in different types of noise jamming, including: barrage, spot and bin masking. We can categorize jamming according the relative location of the jamming vehicle, the vehicle being shielded, and the radar—thus defining Stand-in and Stand-off jamming [4]. Stand-in jamming of radar implies the jammer is between the shielded vehicle and the radar, whereas Stand-off jamming means the shielded vehicle is closer to the radar than the jammer. Jamming can also be either Escort, where a special jamming aircraft fly with aircraft that are to be shielded, or Self-protection, where an aircraft is able to supply its own jamming support [4]. The effect of jamming can be seen in Figure 2.

Since the radar energy spreads over an increasingly large area as it travels out to a target, the energy that reaches a target is inversely proportional to square of the range. This same phenomenon is at work for the energy reflected from the target back to the radar. Thus, the energy reflected back to a radar is inversely proportional to range to the fourth power, defined here by R4.

Figure 2 shows a return signal from a target which is inversely proportional to 1R4. Also note the two noise levels: the lower level represents the noise inherent in a radar output (due to electrical sources and environmental clutter); the high level represents noise level output by a radar when jamming is being used. Where the target signal rises above the nominal noise at a range of about 1.8 units, the target would be able to approach the radar to about 1.25 units before being detected, if jammed. One reason jamming can be effective is that the jamming vehicle has a mathematical advantage that is proportional to the square of the range. From Figure 3 we can see how detection range is affected by radar proximity with the jammer and target. Again, the effect of jamming is to reduce the burn-through radius of the radar.

If we must fly a strike aircraft near a radar site to hit targets, we'll often want to use a jamming aircraft to jam the radar, as shown in Figure 4. Here we see the radar site as a dot inside concentric rings, and the strike vehicle path as the line from the start to the destination. The outermost ring designates the nominal (un-jammed) radar detection radius. The innermost circle represents the minimum radius the strike aircraft requires. The dotted ring will vary in size and indicates that jamming requirements are functions of strike aircraft location, and thus time. Therefore, the jamming requirements are a time dependent EM power allocation problem for the jammers.

False Target Generation amounts to sending signals to the radar that would be expected if targets were in predefined locations. For an aircraft to make a radar see multiple targets at ranges beyond the its own position, it simply sends delayed signals back to the radar using transponders or repeaters, which send back the type of signal the radar expects. To

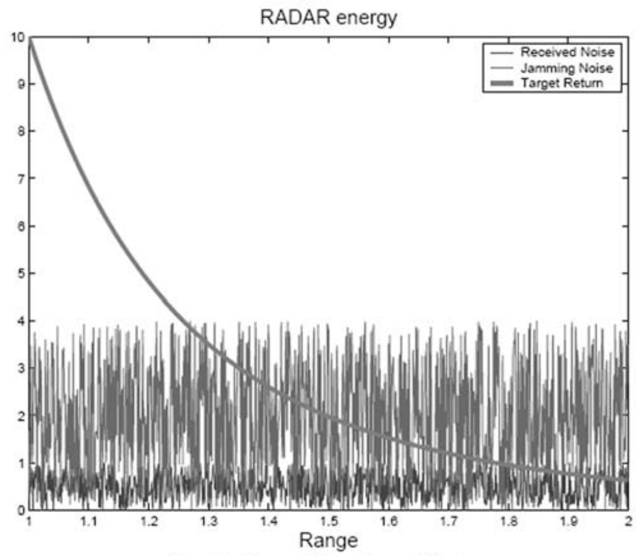

Fig. 2. Target Signal and Noise

insure this, devices called Digital Radio Frequency Memory (DRFM) record a digital representation of the signal, to insure maximum fidelity of the signals transmitted back to the radar. If the aircraft anticipates a certain signal structure, we can send another signal in advance of the incoming radar illumination, causing the radar to see targets at closer range than that of the actual aircraft. However, since many of today's radar systems are pulse-to-pulse agile, they are able to change their pulse characteristics, preventing one from confidently anticipating pulse structure. In this case, the jamming aircraft would need to be closer to the radar than the false targets being created. To be believable to an enemy, the range of the false target would need to be within the burn-through-radius of the radar, which in turn requires the jamming aircraft to be within this range—thus vulnerable to threats.

It is also possible to make radars see targets at angles different from the line-of-sight to the jamming aircraft. To achieve this, the jamming aircraft sends EM into a sidelobe of the radar. Since the radar assumes reflected energy is returning through its main beam, the angle to the perceived target is different than the line from the radar to the jamming aircraft. To use this angle deception, the jamming aircraft locate of the main beam so that energy can be consistently sent into the same sidelobe. Given the side lobe's lower gain, the jamming aircraft must be able to supply enough energy to overcome the attenuation.

The issue of sidelobe jamming requires the jamming aircraft to know its LOS with respect to the radars' mainbeam and lobe structure to maintain an angular orientation that will fool the radar. It also requires the jamming aircraft to maintain a distance from the radar that allow sufficient EM energy to enter the radar receiver. Thus, in the context of control, we have a path planning problem. Our ability to generate false targets at ranges beyond the range of the jamming aircraft—and within the main beam and sidelobes of the radar—can produce a large number of false targets to confuse a radar system.

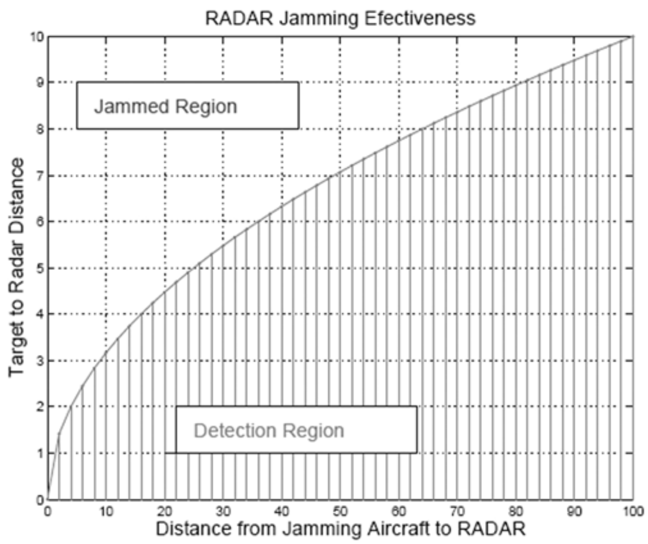

Fig. 3. Jamming Effectiveness

The cooperative nature of this part of the control problem, is that of correlating the false target information sent to one radar by one jamming aircraft, with information sent by other jamming aircraft to different radar systems, all of which overlap the same area. If we ignore this, an IADS radar system could discard the track, because it provides inconsistent information.

Cooperative Control Of UAVs

Cooperative control of UAVs is an active area of research, resulting in a variety of applications, problem formulations and algorithms. McLain and Beard address a cooperative rendezvous problem where multiple UAVs attempt to minimize accumulated exposure to radars, while attempting to rendezvous at a specified location at the same time.[5] Their approach relied on path refinement to generate flyable paths, and path deviations were added to consume slack time and make vehicles arrive simultaneously. Notably, biologically inspired research from "swarm" behaviors led to stability theorems and path planning algorithms applicable to UAVs.[8] Stochastic Dynamic Programming has been used to produce paths for cooperative search using UAVs.[9] The challenge is the cooperative control areas become formulations of a constrained optimization problem, where one is attempting to derive algorithms that minimize time, fuel, threat exposure, or to maximize the performance, duration, and coverage.

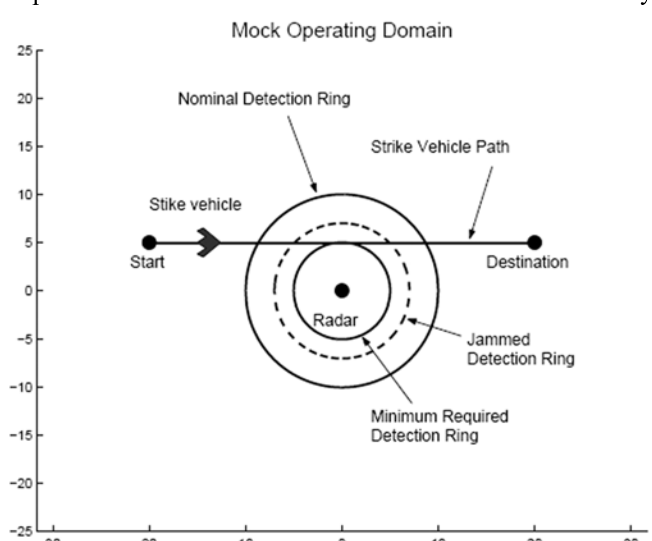

Fig. 4. Strike Aircraft Flying Near RADAR

Although the research mentioned above has no direct link to EA, they show a similar optimization problem. Our motivation is to consider technology that could, with considerable additional development, be used on existing and future UAVs. More specifically, we can apply existing algorithms and develop new ones for generic, highly abstracted scenarios involving teams of unmanned Electronic Combat Air Vehicles (ECAVs) acting against radar system networks.

UAV Role In EA

Use of multiple unmanned air vehicles (UAVs) to deceive radar systems is a relatively new area of study within the broader context of cooperative control and cooperative path planning. Use of small UAVs (tens to hundreds of pounds gross weight), military funding of larger UAV platforms, and potential use of unmanned decoy platforms to deliver EM has spurred interest in how we might use multiple vehicles for EA. With greater capabilities for autonomous operation emerging, cooperative and coordinated actions of groups of UAVs could have a synergistic effect.

Since UAVs can be smaller and have reduced safety considerations, they have the potential to change the complexion of the EA. Smaller sizes can not only make UAVs more stealthy and less vulnerable to enemy weapons, they can be considerably cheaper alternatives to manned aircraft.

There are a number of tactics for performing EA using EW aircraft acting independently or "loosely coupled." However, we could broaden the variety of EA entities to include UAVs acting with one another, as well as within a larger framework. Since UAVs are cheaper, they may present a low cost part of EA within a "system of systems" approach. Teams of UAV stand-in jammers in close proximity to radars could be very effective, *if* they are able to coordinate their activities and positions with one another and with other EA systems. But to make UAV teams a good solution, all associated costs must be kept low. Alternately, a drawback to smaller EA assets with low unit costs is that each unit will also have less capability. The amount of EM power produced by each vehicle, the frequency options, and the ability to direct EM will likely be much less than conventional manned platforms. However, due to the quadratic benefit of range, UAV jamming may be of greater importance.

Intelligence Preparation of the Battlespace (IPB) provides information regarding location of enemy assets [10] such as radar sites, however, we must assume mobile radars will pop-up without warning during a SEAD mission. The likelihood and number of these types of events would also be provided with the enemy assessment part of the IPB. Mobile sites are

Contemplating a sky full of UAVs. (US Marine Corps)

generally triggered when prompted by other radars. Part of the UAV's utility is using them as decoys—without placing people in harm's way—causing an adversaries to turn on their radars, thus giving away their locations.

Choreographed into an EA plan, UAVs would help obtain accurate information, and provide additional degrees of freedom for SEAD planners. However the larger solution space, without guidance for optimal use, could be no benefit or simply add to the "fog of war." Therefore, we require tools not just for UAV use, but for all EA system layers. Because solution to the greater EA problem involves many assets, the ensuing optimization problem would likely be too unwieldy to attack in its entirety. We would need a set of integrated algorithms and heuristics to address this.

Key Areas

Within non-destructive, non-lethal SEAD there are two basic approaches: deception (sometimes called technique jamming); and EM (as noise seen by the radar) jamming. UAVs could provide a means for achieving many EA goals, however algorithmic solutions would need to be incorporated that are capable of working within the computational limits imposed by a UAV.

Both of the SEAD methods above assume we know radar locations and characteristics, but unknown or mobile radars will almost always complicate the EA problem. However, UAVs could play an information gathering role looking for unknown radars, plus we could take advantage having additional UAVs in the battlespace. By cooperatively positioning UAV orbits and fusing observations, we minimize the ellipse of error probability. Multiple vehicles provide improved threat direction information, and UAV decoys could be used to distract radars or cause unknown enemy EM assets to switch on and reveal their locations.

As we go on to describe other deception and noise jamming problem possibilities, it is important to note these discussions may or may not have immediate operational relevance. There may be better uses for assets positioned reasonably close to the enemy. However, these formulations provide a means for defining cooperative control problems which are pervasive for use of UAVs in EA.

Deception

For the deception, we consider two different problem formulations where Electronic Combat Air Vehicles (ECAVs) are used create Phantom tracks (radar target trajectories which do not really exist). In figure 5 we see four ECAVs using time delay of the return radio frequency signal, to deceive four radar sites into believing that a Phantom aircraft exists beyond the ECAVs. We'll assume the ECAVs are stealthy (unseen by the radar), are able to direct a return signal to one of the radars that will not affect the other three radars, and the radars are assumed to correlate their information. The trajectory (track) of the Phantom is shown as a continuous path, and the control problem is one of ECAV path planning where the geometry largely dictates the ECAV trajectories, i.e. the ECAVs are required to remain on the LOS between one radar and the Phantom. Two points on the Phantom path are noted at times t(1) and n steps later at t(n + 1) to illustrate how the geometry influences the ECAV paths. As long as we use realistic velocity limits and vehicle dynamics, the ECAVs are free to position themselves on the LOS like beads on a string. This model abstracts the radar electronics, leaving a tightly coupled path planning problem.

The geometry of one UAV and one radar with respect to a reference azimuth is shown in Figure 6. The trigonometric relationships show the Phantom and ECAV angular rate and range rate in terms of velocity vectors. From the geometry of this figure, one can show that the radar can be induced to see a desired Phantom velocity vector by an infinite number of ECAV velocity vectors. If one assumes a constant ECAV speed, then the a desired Phantom velocity vector results in a uniquely determined angle, µE. If we put constraints on the ECAV turn rate and velocity, there will be annular regions

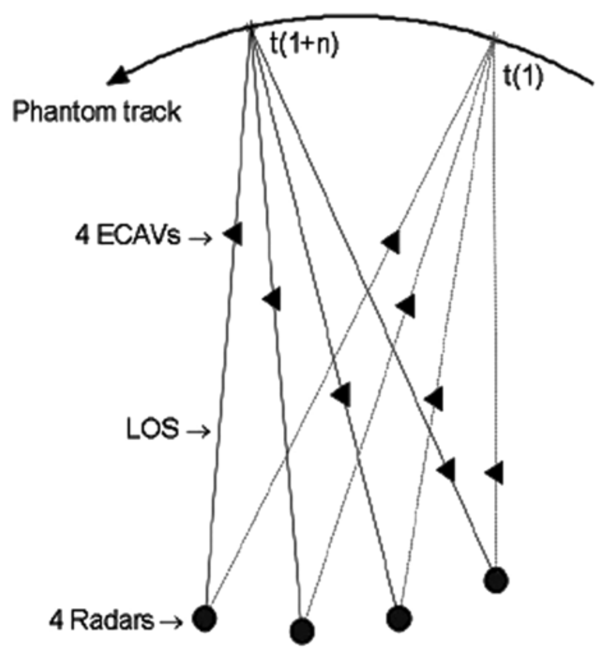

Fig. 5. Deception of 4 RADARs using 4 ECAVs

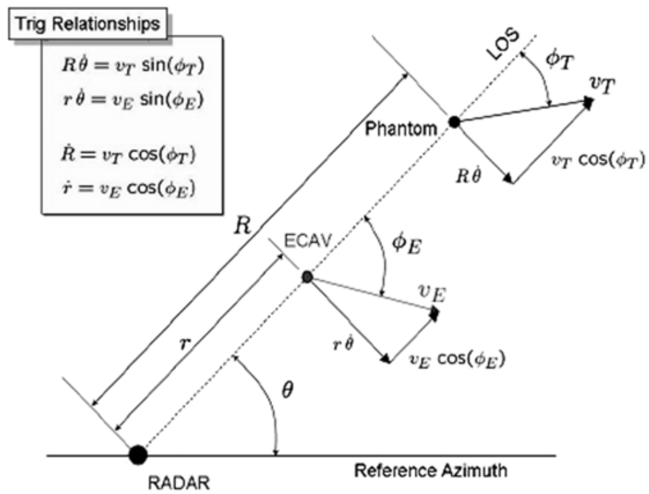

Fig. 6. Deception Problem Geometry

where the Phantom could fly within a defined time step. In the first of the two approaches defined here, we desire an optimal combination of Phantom and ECAV trajectories, while in the second approach, we wish to find a feasible solution. In both cases we assume that the necessary information is communicated without error or delay.

However, for the feasible solution approach, the information needed is considerably less than that required for the optimal approach. Both approaches assume that velocity constraints exist for both the ECAVs and Phantom, and that the dynamics of the ECAVs impose turn rate restrictions. Both sets also assume the ECAVs start at locations that give them a coherent Phantom track, i.e. one that is correlated for each radar, and that the ECAVs delay the radar signal by the proper amount of time to place the Phantom at the correct range. This leads us to our optimal approach: a path planning control algorithm which has each ECAV maintain a path on its own radar-Phantom LOS, with the smallest possible cost. Again, this currently neglects issues relating to communication of information between ECAVs. Thus, each ECAV operates in a decentralized, but redundant fashion, using global information.

To provide an optimal solution to the deception problem, we define a cost function that includes terms that penalize undesirable characteristics of both the Phantom track and the ECAV tracks. In qualitative terms, this approach allows the ECAVs to negotiate a solution which produces believable Phantom tracks, is able to do so for a long period of time, and does not make excessive demands on the ECAV dynamics. To obtain the results described here, a receding horizon approach was taken where an optimal set of ECAV paths was computed for a prediction horizon of predefined length, and then flown for a fraction of that time (the control horizon).

To understand the rationale behind the cost function used let us first consider the geometry shown in figure 7. This figure shows three radars, the Phantom, and three ECAVs on the radar-Phantom LOS. We want the radars be deceived into thinking the Phantom flies through the waypoint on its way to the endpoint. Because constraints can sometimes make it costly to exactly follow prescribed paths or hit waypoints precisely, we define a broader waypoint region. From a modeling standpoint, this is more acceptable than constraint violation or extremely high costs [11].

So what is the most feasible approach? How do we determine what could be done if our planners are willing to settle for solutions which are feasible, but not necessarily optimal? [12]. Such an approach would require less inter-UAV communication, which might be better in some operational contexts. The objective of a feasible solution is to create the same type of coherent Phantom track described for the optimal approach above and depicted in Figure 5, however only feasibility with respect to dynamic and velocity constraints are considered. As seen in Figure 6, given the present position of the Phantom, the present position and orientation of an ECAV, a maximum and minimum velocity magnitude and direction of the ECAV, and using the relationship shown in equation 2, one can calculate an annular region where the Phantom could feasibly be positioned within a given time step. In order to move a Phantom from an initial position to a waypoint or final destination, each ECAV communicates four numbers (minimum and maximum ECAV angle and velocity) with each other ECAV. Each ECAV then uses this information to calculate the intersection of the annular regions. By choosing the direction closest to the direct path to the waypoint (or destination), the Phantom moves in the desired direction.

Such a solution degenerates to a straight line path from start to finish if such a Phantom path is feasible for all the ECAVs. Figure 8 shows results of a simulation where four ECAVs are deceiving four radars into seeing a Phantom track moving from a starting point to a final destination. In Figure 8, the Phantom track and ECAV trajectories are shown and dotted lines are shown as LOS between the radar and Phantom for the start and final points of the track. For the first segment of the simulation,

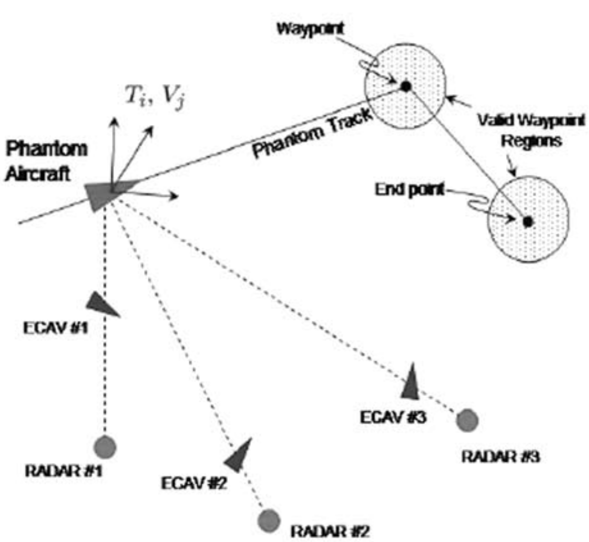

Fig. 7. Optimization Problem Geometry

$$J_C(\psi_i, V_j) = J_P(\psi_i, V_j) + \sum_k J_{E_k}(\psi_i, V_j)$$

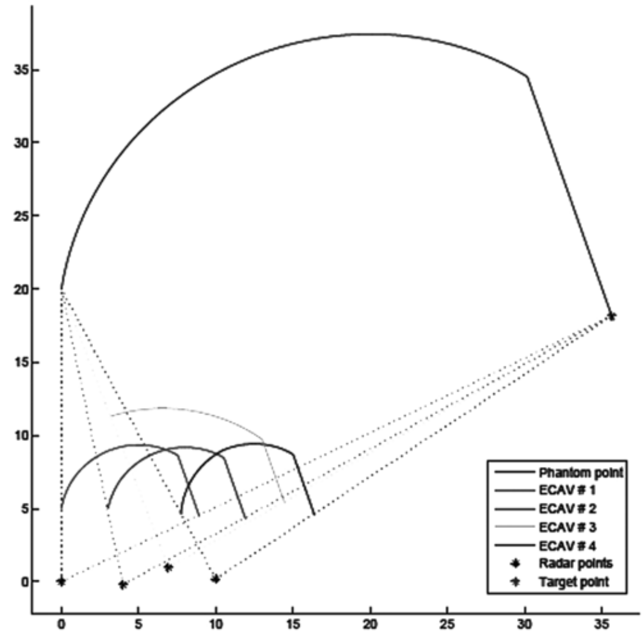

Fig. 8. Feasible Solution for Phantom Trajectory Generation

the Phantom trajectory is a sequence of small line segments forming an arc. However, once the ECAVs reach positions and orientations that allows them to induce a straight line Phantom trajectory to the destination, the Phantom trajectory becomes a straight line. Details of this work can be found in [12].

Conclusion

This has been a brief background and operational context for applying UAVs to the Electronic Attack problem, describing just a few of the technical challenges involved. We have explored cooperative control of UAV groups or "swarms" within the context of some abstract EA scenarios, but more modeling and testing are vital. Relevant issues not addressed include imperfect communications—where only local information or corrupted information is available for decisions—or for planning and control. Again, UAVs for EA will most often be part of a larger EA framework using multiple vehicles. However, a complete EA solution hierarchy utilizing many types of vehicles will make for a large optimization problem, requiring decomposition into a number of smaller problems. Finally, there is a plethora of research and development in the area of radar electronics which is very important for a comprehensive treatment of EA. The scenarios here are not meant to be of immediate operational significance, but to illustrate salient features. Cooperative control of UAVs for Electronic Attack offers plenty of potential.

References

[1] *JTTP for Joint Suppression of Enemy Air Defenses*, July 1995, http://www.dtic.mil/doctrine/jel

[2] G. Stimson, *Introduction to Airborne radar*. Scitech, 1998.

[3] *Joint Doctrine For Electronic Warfare*, April 2000,http://www.dtic.mil/doctrine/jel

[4] J. A. Tirpack, "The New Way Of Electron War," *Air Force Magazine*, December 2004.

[5] T. McLain, "Cooperative Rendezvous Of Multiple Unmanned Air Vehicles," AIAA Guidance, Navigation, and Control Conference, August 2000.

[6] K. Nygard, P. Chandler, and M. Pachter, "Dynamic Network Flow Optimization Models For Air Vehicle Resource Allocation," Proceedings of the Automatic Control Conference, June 2001.

[7] C. Schumacher, P. R. Chandler, and S. R. Rasmussen, "Task Allocation for Wide Area Search Munitions Via Iterative Network Flow," Proceedings of the American Control Conference, pp. 1917–1922,2002.

[8] V. Gazi and K. M. Passino, *"Stability Analysis of Swarms in an Environment With an Attractant/Repellent Profile," Proceedings of the American Control Conference*, pp. 1819–1824, 2002.

[9] M. Flint, M. Polycarpou, and E. Fernandez-Gaucheand, "Cooperative Control For Multiple Autonomous UAVs Searching For Targets," Conference on Decision and Control, pp. 2823–2828, 2002.

[10] L. C. M. T. Satterly, L. C. D. Stubbs, M. G. D. Gilbert, M. C. L. Iler, and C. K. B. Glen, "Intelligence Preparation of The Battlespace - An Airman's Introduction," *Air and Space Power Chronicles* - Chronicles Online Journal, July 1999.

[11] M. J. Mears and M. R. Akella, "Deception of Radar Systems Using Cooperatively Controlled Unmanned Air Vehicles," International Conference on Networking, Sensing and Control, March 2005.

[12] D. Maithripala and S. Jayasuriya, "Radar Deception Through Phantom Track Generation," *Proceedings of the American Control Conference*, June 2005.